AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A system of managing ~~the~~ security ~~of~~ for data processing applications, comprising:

~~directory files~~ directories in which the data processing applications are stored, said ~~directory files~~ directories being organized in an n-level tree~~, the level 1 directory being the highest level~~; and

a number of security registers which ~~can each be allocated to a single directory~~ are selectively allocatable to any one of a plurality of said directories, each security register containing all ~~the~~ rights or secrets which have been granted under ~~a~~ the directory to which it has been allocated.

2. (Currently Amended) A method of managing ~~the~~ security ~~of~~ for data processing applications, comprising the steps of:

dynamically allocating a security register to one of a plurality of directories that are organized in an n-level hierarchy;

~~(a)~~ storing in an allocated security ~~registers the~~ register rights granted under ~~a~~ the directory to which said register has been allocated, according to given rules;

~~(b)~~ seeking the secrets presented in ~~an n-level tree of directory files~~ a directory in which a data processing ~~applications are~~ application is stored; and

(c) verifying the knowledge of one or more rights at the level of ~~the~~ said data processing application.

3. (Currently Amended) A method according to claim 2, wherein ~~the storage rules of step (a) are as follows~~ said allocating step is performed according to the following rules:

allocation of a security register to a current directory as soon as a right has been granted under this directory or said security register has been updated if a right has already been granted under this directory;

~~loss of the link connecting the old~~ removing the allocation of a security register to a current directory ~~to its security register~~ when a new directory is selected except if the selected new directory is ~~the~~ a child of the ~~old~~ current directory; and

allocating the security register that was allocated the earliest to ~~the new current~~ a new directory if the security registers are all allocated.

4. (Currently Amended) A method according to claim 2 wherein said seeking step ~~(b) consists of applying~~ is performed according to the following rule:

verifying that ~~the~~ a secret presented is known in ~~the~~ a current directory (Ni) or in a directory at a higher level of the hierarchy.

5. (Currently Amended) A method according to claim 2, wherein said seeking step ~~(b)~~ comprises the following intermediate steps:

~~(b1)~~ seeking a secret in the current directory at level (Ni) and verifying the existence of the secret within the application;

~~(b2)~~ if said secret exists, verifying that ~~the~~ presentation of the secret has succeeded;

if the presentation has succeeded, granting the right associated with the secret ~~is granted~~ at the level (Ni) of the current application;

if the presentation has failed, refusing to grant the right associated with the secret ~~is not granted~~ and terminating the attempted presentation ~~is terminated~~;

~~(b3)~~ if said secret does not exist within the current application at level (Ni), ~~seeking~~ determining whether this secret exists within the parent application at level N(i-1);

~~(b4)~~ if said secret exists in the parent application at level N(i-1), verifying that the presentation has succeeded;

if the presentation has succeeded, granting the right associated with the secret ~~is granted~~ in the current application at level (Ni);

if the presentation has failed, refusing to grant the right associated with the secret ~~is not granted~~ and terminating the attempted presentation ~~is terminated~~;

~~(b5)~~ if the secret does not exist within the parent application at level N(i-1), seeking the existence of the secret at the level of the application at level N(i-2) ~~along the hierarchical axis~~ within the hierarchy and verifying that the presentation has succeeded;

and so on as far as the highest hierarchical level as long as the existence of the secret has not been discovered;

~~(b6)~~ if the secret has not been discovered, terminating the attempted presentation ~~is terminated~~.

6. (Currently Amended) A method according to claim 2, wherein the verifying step ~~(c) consists of applying~~ is performed according to the following rule:

authorization of a function requiring knowledge of a secret if and only if, ~~running through the tree along the hierarchical axis~~ within the hierarchy from the current application to the root application, ~~the~~ a first secret is known to at least one of the applications ~~belonging to the tree section~~ along a path in the hierarchy for which the current application and the application containing the secret are delimiters.

7. (Currently Amended) A method according to claim 2, wherein said verifying step ~~(c)~~ comprises the following steps:

~~(c1)~~ verifying that a security register is associated with ~~the~~ a current application at level Ni;

~~(c2)~~ authorizing ~~the~~ a function if the security register contains ~~the~~ a required right and terminating the verification;

~~(c3)~~ seeking the existence of ~~the~~ a reference secret within the current application at level Ni if no security register is associated with the current application or if the associated register does not contain the required right;

~~(c4)~~ refusing the function and terminating the verification if the secret exists within the current application;

~~(c5)~~ verifying that a security register is associated with the parent application at level N(i-1) of the current application if the reference secret does not exist within the current application at level Ni;

~~(c6)~~ authorizing the function and terminating the verification if the security register associated with the parent application contains the right required for using the function;

~~(c7)~~ seeking the existence of the reference secret within the parent application at level N(i-1) of the current application if no security register is associated with the parent application or if the associated security register does not contain the required right;

~~(c8)~~ refusing the function and terminating the verification if the reference secret exists within the parent application at level N(i-1);

~~(c9)~~ verifying that a security register is associated with the grandparent application at level N(i-2) of the current application along ~~the hierarchical axis of~~ a path within the hierarchy from the current application towards the root application, if the reference secret does not exist within the parent application at level N(i-1);

and so on as long as the existence of the reference secret has not been discovered; and

~~(c10)~~ refusing the function and terminating the verification if the secret has not been discovered.